



217 #2

520.41126X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): KAIJYU, et al

Serial No.: 10 / 058,778

Filed: JANUARY 30, 2002

Title: FILE TRANSMITTING METHOD AND SYSTEM

RECEIVED
MAR 08 2002
Technology Center 2100

LETTER CLAIMING RIGHT OF PRIORITY

Assistant Commissioner for
Patents
Washington, D.C. 20231

MARCH 7, 2002

Sir:

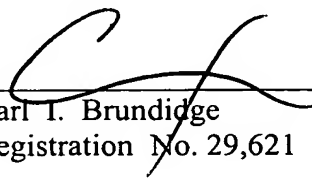
Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s)
the right of priority based on:

Japanese Patent Application No. 2001-261774
Filed: AUGUST 30, 2001

A certified copy of said Japanese Patent Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Carl I. Brundidge
Registration No. 29,621

CIB/rp
Attachment

NT059403



日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2001年 8月30日

RECEIVED

MAR 08 2002

出願番号

Application Number:

特願2001-261774

Technology Center 2100

ST.10/C]:

[JP2001-261774]

出願人
Applicant(s):

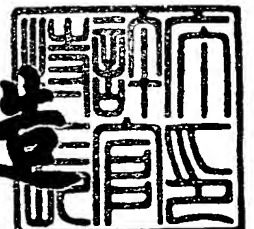
株式会社日立製作所
株式会社 日立システムアンドサービス

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 2月 1日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 KN1354

【提出日】 平成13年 8月30日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00

【発明者】

 【住所又は居所】 東京都大田区大森北三丁目2番16号 株式会社 日立
システムアンドサービス内

 【氏名】 海住 高広

【発明者】

 【住所又は居所】 神奈川県川崎市幸区鹿島田890番地 株式会社 日立
製作所 金融システム事業部内

 【氏名】 山岸 崇志

【発明者】

 【住所又は居所】 東京都大田区大森北三丁目2番16号 株式会社 日立
システムアンドサービス内

 【氏名】 的場 哲夫

【発明者】

 【住所又は居所】 神奈川県川崎市幸区鹿島田890番地 株式会社 日立
製作所 金融システム事業部内

 【氏名】 神谷 政美

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社 日立製作所

【特許出願人】

 【識別番号】 391002409

 【氏名又は名称】 株式会社 日立システムアンドサービス

【代理人】

 【識別番号】 100078134

【弁理士】

【氏名又は名称】 武 顕次郎

【電話番号】 03-3591-8550

【手数料の表示】

【予納台帳番号】 006770

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003102

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ファイル伝送方法及びファイル伝送システム

【特許請求の範囲】

【請求項1】 インターネットを介して、クライアントとサーバとの間でファイルデータを伝送するファイル伝送方法において、ファイルデータの伝送を専用プログラムを用いるHTTPSプロトコルを使用して行うことを特徴とするファイル伝送方法。

【請求項2】 前記伝送されるファイルデータは、一定サイズに分割されたファイルデータとされており、そのデータが圧縮されていることを特徴とする請求項1記載のファイル伝送方法。

【請求項3】 前記分割されたファイルデータに、チェックポイントが付与されており、障害発生時、前記チェックポイントを使用してファイルデータを、そのチェックポイントから再送することを特徴とする請求項2記載のファイル伝送方法。

【請求項4】 前記専用プログラムは、マルチプラットフォームに対応させられており、クライアントのオペレーションの延長でサーバからダウンロードされることを特徴とする請求項1、2または3記載のファイル伝送方法。

【請求項5】 前記専用プログラムには、製造元を明確にする電子証明書が付加されていることを特徴とする請求項4記載のファイル伝送方法。

【請求項6】 前記専用プログラムを動作させるための設定情報が、サーバからクライアントにダウンロードされることを特徴とする請求項1ないし5のうちいずれか1記載のファイル伝送方法。

【請求項7】 前記HTTPSプロトコルには、専用プログラムのバージョン管理機能、ファイルのアップロード機能、ファイルのダウンロード機能、ファイルデータの分割転送機能、転送データの圧縮機能、チェックポイントからの再送機能、タイマ監視機能のうち少なくとも1つが実装されていることを特徴とする請求項1ないし6のうちいずれか1記載のファイル伝送方法。

【請求項8】 インターネットを介して、クライアントとサーバとの間でファイルデータを伝送するファイル伝送システムにおいて、ファイルデータの伝送

を H T T P S プロトコルを使用して行う専用プログラムを備えることを特徴とするファイル伝送システム。

【請求項 9】 前記専用プログラムは、マルチプラットフォームに対応させられており、製造元を明確にする電子証明書が付加されていることを特徴とする請求項 8 記載のファイル伝送システム。

【請求項 1 0】 前記 H T T P S プロトコルには、専用プログラムのバージョン管理機能、ファイルのアップロード機能、ファイルのダウンロード機能、ファイルデータの分割転送機能、転送データの圧縮機能、チェックポイントからの再送機能、タイマ監視機能のうち少なくとも 1 つが実装されていることを特徴とする請求項 8 または 9 記載のファイル伝送システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、ファイル伝送方法及びファイル伝送システムに係り、特に、インターネット環境下におけるクライアント P C と W e b サーバとの間でファイルの伝送を行うファイル伝送方法及びファイル伝送システムに関する。

【 0 0 0 2 】

【従来の技術】

インターネット環境下におけるクライアント P C と W e b サーバとの間でファイルの伝送に関する従来技術として、① F T P プロトコルを使用してファイル伝送を行う、② H T M L の入力フォームの指定によりファイル送信を行う、③クライアント P C に専用プログラムをインストールし、この専用プログラムを使用してファイル伝送を行うという方法が知られている。

【 0 0 0 3 】

①の F T P プロトコルを使用する方法は、例えば、クライアント P C のローカルファイルを、社内イントラネット上の W e b サーバのファイルへアップロードする場合、そのアップロードを可能にするために、社内イントラネットの入り口に設けられる F W (ファイアウォール) を、アップロード可能に設定する必要がある。

【0004】

また、②のHTMLの入力フォームの指定による方法は、通常、FWを通過することができるプロトコルが、そのセキュリティ上HTTPに限定されているので、HTMLで標準に規定している入力フォームの指定により、ファイルの伝送を実現させなければならない。

【0005】

また、③のクライアントPCに専用プログラムをインストールし、この専用プログラムを使用する方法は、クライアント・サーバ間で、HTTPプロトコルに、独自のファイル伝送プロトコルをトンネリングさせるというもので、ファイル伝送プロトコルに、ファイルデータの分割送信等の機能実装することにより、長大なファイルを送信した場合にも、サーバ側アプリケーションプログラムが、メモリ常駐しているので、サーバ側の負荷が高くなるということを防止することができるという利点を有している。

【0006】

【発明が解決しようとする課題】

前述した①の従来技術は、FWをアップロード可能に設定して、不特定のIPアドレスからのFTPのアップロードを許しているため、悪意のある第三者が、大量のデータを送りこんでサーバ内のディスクをパンクさせ、サーバをダウンさせられる場合が生じるという問題点を有している。

【0007】

また、②の従来技術は、クライアントからサーバへのファイルの伝送が、ファイルサイズそのままの大きさで行われるため、ファイルが大きくなるほど、サーバ側のアプリケーションプログラムがファイルデータを読み込んでファイルを出力するまでのメモリ常駐時間が長くなり、サーバ負荷が大きくなってしまいう問題点を有している。

【0008】

さらに、③の従来技術は、ファイルのアップロード機能、ファイルのダウンロード機能、ファイルデータの分割転送機能、転送データの圧縮機能、ファイルのアップロード、ダウンロード異常終了時のチェックポイントからの再送機能、タ

イマ監視機能等の大きく機能を持たせた専用プログラムを、予め、ブラウザPCにインストールしておかなければならず、この専用プログラムとして、クライアントPCのプラットフォームに応じたものを用意しなければならないという問題点を有している。また、この従来技術は、クライアントPC毎に、専用プログラムのインストールが発生し、ユーザの操作が面倒になるため、インターネットにおける普及の妨げとなるという問題点を有している。

【0009】

本発明の目的は、前述した従来技術の問題点を解決し、不安定がちなインターネットを使用して、クライアントPCで、特別な操作をすることなく、世界的に広く普及しているHTTPSプロトコルを使用し、かつ、長大ファイルの送受信を高い信頼性を持って効率よく行うことが可能なファイル伝送方法及びファイル伝送システムを提供することにある。

【0010】

【課題を解決するための手段】

本発明によれば前記目的は、インターネットを介して、クライアントとサーバとの間でファイルデータを伝送するファイル伝送方法において、ファイルデータの伝送を専用プログラムを用いるHTTPSプロトコルを使用して行うことにより達成される。

【0011】

前述において、ファイルデータは、一定サイズに分割されたファイルデータとされ、データが圧縮されて伝送され、また、分割されたファイルデータには、チェックポイントが付与されて、障害発生時、前記チェックポイントを使用してファイルデータが、そのチェックポイントから再送される。

【0012】

【発明の実施の形態】

以下、本発明によるファイル伝送方法及びファイル伝送システムの実施形態を図面により詳細に制御する。

【0013】

図1は本発明の一実施形態によるファイル伝送システムの全体の構成を示すブ

ロック図、図2は専用プログラム動作環境の設定について説明する図、図3は専用プログラムのダウンロードについて説明する図である。図1～図3において、10はクライアントPC、11はバッチファイル、12は設定情報ファイル、13、22は専用プログラム、14はプラグイン手段、15は転送ディレクトリ、16、36は転送ファイル、20はWWWサーバ、21はバッチファイル、23はサーバ側アプリケーションプログラム、24はWWWサーバプロダクト、30は端末運用WWWサーバ、31はWWWサーバプロダクト、32は運用端末アプリケーション、33はアプリケーション（AP）サーバ、34はファイルサーバ、35は契約情報ファイル、40はインターネット、41はターミナルアダプタ、42はルータ（R）、50は運用端末である。

【0014】

本発明の実施形態によるファイル伝送システムは、図1に示すように、クライアントPC10と、WWWサーバ20、運用端末サーバ30、APサーバ33、ファイルサーバ34の複数のサーバを含んで構成される処理システムとがインターネット40等のネットワークを介して接続されて構成されている。前述の処理システムを構成する複数のサーバ相互間は、ルータ42を有するLAN等のネットワークを介して相互に接続され、ファイルサーバ34には、クライアントPC10を運用する顧客としての企業単位、利用者単位の契約情報毎にクライアントPC10の設定情報を格納する契約情報ファイル35と、クライアントPC10が持つ転送ファイルとの間でのファイル転送を行うファイルを保持する転送ファイル36とが接続されている。

【0015】

LAN等のネットワークには運用端末50が接続されており、この運用端末50は、前述した契約情報ファイル35に格納する契約情報毎のクライアントPCの設定情報等を入力するために使用され、入力された情報は、運用端末WWWサーバ30におけるWWWサーバプロダクト31、運用端末アプリケーションプログラムを介して契約情報ファイル35に格納される。

【0016】

WWWサーバ20は、クライアントPC10での専用プログラムの動作環境の

設定情報を持つバッチファイル 2 1 と、クライアント PC 1 0 にダウンロードする専用プログラム 2 2 と、サーバ側アプリケーションプログラム 2 3 と、WWWサーバプロダクト 2 4 とを備えて構成される。また、クライアント PC 1 0 は、WWWサーバ 2 0 からの設定情報を受け取っていったん格納するバッチファイル 1 1 と、専用プログラムの動作環境、セキュリティ情報等を格納しておく設定情報格納ファイル 1 2 と、WWWサーバ 2 0 からダウンロードした専用プログラム 1 3 と、プラグイン手段 1 4 と、転送ディレクトリ 1 5 と、ファイルサーバが持つ転送ファイル 3 6 との間でのファイル転送を行うファイルを保持する転送ファイル 1 6 とにより構成され、ターミナルアダプタ 4 1 を介してインターネット 4 0 に接続されている。

【 0 0 1 7 】

前述したように構成されるファイル転送システムは、例えば、金融機関のサーバシステムと企業ユーザ等との間で、振込み情報等の大量のファイル情報を転送するような場合に使用して好適なものであり、金融機関とユーザとの間で、比較的信頼性の低いインターネットを介して、振込み情報等の重要な情報を高いセキュリティ性を持って転送することができるようにしたものである。この場合、図 1 に示す複数のサーバにより構成される処理システムが金融機関に設けられるシステムであり、クライアント PC 1 0 が取引企業等に備えられる端末である。

【 0 0 1 8 】

次に、前述したような本発明の実施形態によるシステムの機能概要について説明する。

【 0 0 1 9 】

本発明の実施形態は、高いセキュリティ性が要求されファイルを確実に転送可能とするために、ハッキング等による妨害を受けることが少ない HTTP プロトコルを使用してファイルの伝送を実現する。このため、図 1 には図示していない処理システムの入り口に設けられるファイアウォール FW が、HTTP プロトコルの通過のみ許可するように設定される。そして、送受信されるファイルデータの盗聴をも防止する意味で、SSL 1 2 8 ビットの暗号化を行う HTTPS プロトコルを使用してファイルの伝送を行う。

【0020】

本発明の実施形態は、前述したようなファイル伝送を行うために、そのための専用のプログラムを使用することとし、予め、専用プログラム動作環境をクライアントPC内に設定するようにする。この専用プログラム動作環境の設定は、専用プログラムが動作するための（ファイル伝送を行う上でファイルアクセスを許可する等の）設定情報を、サーバからダウンロードして、クライアントPCへ自動設定することにより行われる。設定情報は、マルチプラットフォームに対応できるように、ユニックス、ウィンドウズ（登録商標）等の構文の差を吸収するためのテンプレートを外部から設定できるようにされている。

【0021】

前述したように、クライアントに専用プログラムを持たせ、この専用プログラムによりファイルの伝送を行うため、本発明の実施形態は、クライアント・サーバ間でのHTTPプロトコルに、独自のファイル伝送プロトコルをトンネリングさせる機能を持たせる。この独自のファイル伝送プロトコルは、ファイルデータを圧縮、分割して転送する機能を持ち、伝送効率を向上させ、また、分割してファイルを転送する際、障害発生時の再送を行うためのチェックポイントを設けて、不安定なインターネット通信において、再度、先頭からデータ送信を行うような効率の悪いことをしなくてもよいようされている。また、ファイル伝送プロトコルには、前述の他に、クライアントPC専用プログラムのVR管理、ファイルのアップロード、ファイルのダウンロード、タイマ監視等の機能が追加されている。

【0022】

専用プログラムは、サーバからクライアントにダウンロードされるが、ダウンロードする専用プログラムには、電子証明書を付加することによって、製造元を明確にし、不当な書き換え等を発生させないようにする。そして、専用プログラムのダウンロードは、ユーザオペレーションの延長で行うことによって、ユーザに対して手間を掛けさせないようにしている。

【0023】

さらに、本発明の実施形態は、専用プログラムをマルチプラットフォームに対

応させており、これにより、プラットフォーム毎に専用プログラムを持つ必要をなくすることができるようにしている。また、専用プログラムは、クライアントPCのオペレーションの延長でサーバからダウンロードして使用することができるようにインストールを発生させないようにしている。

【0024】

次に、図2を参照して専用プログラム動作環境の設定について説明する。

【0025】

まず、専用プログラムを動作可能とするための設定情報を、企業単位または利用者単位に、企業ID、利用者IDと共にサーバへ保管する。保管される設定情報は、企業単位でクライアントPCの設定が統一されている場合、企業毎の設定だけでよく、利用者単位にクライアントPCの設定が異なる場合、利用者毎に設定される。保管される設定情報は、ファイル伝送を行う上でファイルアクセスを許可する転送ディレクトリファイルを定義するための構文を記述する設定情報テンプレートと、設定情報に埋め込む転送ディレクトリファイル名と、設定情報をクライアントPCへダウンロードしてから、設定情報を設定するためのバッチファイルのテンプレートとしての設定情報自動設定バッチテンプレートであり、これらは、Java（登録商標）により記述される。

【0026】

設定情報の作成に際し、サーバは、前述した保管されている設定情報の設定情報テンプレートと、設定情報に埋め込む転送ディレクトリファイル名とを用い、設定情報テンプレートの情報を元に、転送ディレクトリファイルの情報を挿入して、転送ディレクトリファイルへのアクセス権限、そのURLへのアクセス権限を含む専用プログラムの権限情報の設定のための設定情報を作成する。

【0027】

そして、サーバは、設定情報自動設定バッチを作成する。このバッチの作成は、前述した保管されている設定情報の設定情報自動設定バッチテンプレートと前述で作成した設定情報とにより、設定情報自動設定バッチテンプレートの情報を元に、転送ディレクトリファイルの情報を挿入して、設定情報自動設定バッチを作成し、この情報を設定情報を設定情報格納ファイルとしてのバッチファイル2

1 に格納する。

【0028】

前述した設定情報としての専用プログラムが利用する転送ディレクトリ名やURL名は、企業単位、利用者単位にサーバ側で定義される。これらの設定情報を例示すると、例えば、

```
grant codeBase "http://XXXXXXXX.co.jp/NetBank/" {
    permission java.io.FilePermission "C:TEMP-", "read, write, delete,
    execute" ;
    permission java.net.SocketPermission "XXXXXXXX.co.jp", "accept,
    connect, listen, resolve" ;}
```

等である。この例において、アンダーラインで示した部分が順に、専用プログラムが格納されているURL名称、専用プログラムのアクセスを許可する転送ディレクトリファイル名、専用プログラムの通信を許可するURL名である。

【0029】

クライアントPC10は、前述のようにして作成された設定情報自動設定バッチをサーバのバッチファイル21からダウンロードし、そのバッチを実行することにより、自PC内の設定情報格納ファイル12のユーザポリシーに専用プログラムの権限情報を挿入する。

【0030】

クライアントPC10は、これにより、専用プログラムをダウンロードする前に、サーバに保管されている設定情報をダウンロードして自動設定されたことになり、専用プログラムをダウンロードして動作させる環境が整ったことになる。

【0031】

クライアントPC10は、専用プログラムをダウンロードし、専用プログラムを使用してファイルの伝送を行うが、次に、図3を参照して、専用プログラムのダウンロードについて説明する。

【0032】

サーバは、専用プログラムの生成時、専用プログラムに電子証明書を付加することにより、その専用プログラムの製造元を明確にし、不当な書き換え等を発生

させないようにする。その際、サーバは、グローバルサーバIDを128ビットSSL暗号化したものも付加し、この電子証明書付き専用プログラムを自サーバ内の専用プログラム22として保存する。

【0033】

クライアントPC10での専用プログラムのダウンロードは、ユーザオペレーションの延長で行うことができる。このため、ユーザは、専用プログラムのダウンロード時、専用プログラムの製造元を「ルート証明書要求確認画面」により、確認して「OK」を指示する入力を行うだけで、特に、専用プログラムをインストールするという煩わしい作業を必要とせずに、サーバ内の専用プログラムを、自PC内の専用プログラム13として取り込むことができる。

【0034】

ユーザは、前述したようにしてクライアントPC10にダウンロードされた証明書付き専用プログラムを起動することにより、自PC10内の転送ファイル16とファイルサーバ34の転送ファイル36との間でのファイルの伝送を、専用プログラムを使用して行わせることができる。

【0035】

本発明の実施形態は、すでに説明したように、クライアントに専用プログラムを持たせ、この専用プログラムによりファイルの伝送を行うため、クライアント・サーバ間でのHTTPプロトコルに、独自のファイル伝送プロトコルをトンネリングさせる機能を持たせており、次に、それらの機能について説明する。

【0036】

1. クライアントPC専用プログラムVR管理

クライアントPCは、専用プログラムをダウンロードすると、一旦、クライアントPC側で保存する。そのため、クライアントPCとサーバとに、専用プログラムのバージョン番号を持たせて管理する。クライアントPCが、専用プログラムを起動すると、サーバ側への問合せを行い、サーバからバージョン番号を応答してもらう。クライアントPCの専用プログラムは、応答されたバージョン番号とクライアントPCで保持しているバージョン番号とが不一致の場合、一旦、終了し、サーバから新しいバージョン番号の専用プログラムをダウンロードする。

【0037】

2. ファイルのアップロード

クライアントPCが、指定したファイルをサーバへアップロードする機能であり、通信には、HTTPSを使用する。

【0038】

3. ファイルのダウンロード

クライアントPCが、指定したファイルにサーバからファイルをダウンロードする機能であり、通信には、HTTPSを使用する。

【0039】

4. ファイルデータの分割転送

ファイルを送信する際にファイルを分割して、一定時間間隔で送信する機能である。分割するサイズ、間隔は、サーバ側で保持している情報に従う。

【0040】

5. 転送データの圧縮

ファイルを転送する際にデータの圧縮を行う機能である。データの圧縮を行うか否かは、サーバ側で保持している情報、または、ファイル伝送を開始する際に、オペレーションにより指定することができる。

【0041】

6. ファイルのアップロード、ダウンロードの異常終了時のチェックポイントからの再送

ファイル転送中に、障害が発生した場合、障害発生前の状態をサーバ側で、保持しており、そのファイルの再送を行う機能であり、ファイルの再送がクライアントPCから指示された場合、サーバで受信済みのデータの次のデータからの送信を行うことができる。

【0042】

7. タイマ監視

ファイルの伝送は、クライアントPCからの問合せ応答により行われるが、応答データが監視時間内に返ってこない（無応答の）場合、ファイル転送を終了させる。

【0043】

図4はクライアントPCが1企業1利用の場合の専用プログラム動作環境設定の処理動作を説明するフローチャート、図5はクライアントPCが1企業複数利用の場合のクライアントPCでの専用プログラム動作環境設定の処理動作を説明するフローチャートであり、次に、これらについて説明する。図4、図5に示すフローは、図2によりすでに説明しているものである。まず、図4のフローを説明する。

【0044】

(1) クライアントPCからファイル伝送の開始が指示されると、サーバは、クライアントPCからのID等の情報を受け、設定情報自動設定バッチの作成とダウンロードとの処理を開始し、まず、利用者単位に設定情報があるか否かを判定する(ステップ401、402)。

【0045】

(2) ステップ402の判定で、利用者単位の設定情報がない場合、サーバ内に格納されている企業IDの設定情報を取得し、利用者単位の設定情報がある場合、利用者IDの設定情報を取得する(ステップ403、404)。

【0046】

(3) サーバは、取得した設定情報を使用して、図2を参照して詳細を説明したように、クライアントPCに設定する設定情報と、設定情報自動バッチとを作成する(ステップ405、406)。

【0047】

(4) その後、サーバは、設定情報自動バッチをクライアントPCにダウンロードして処理を終了する(ステップ407、408)。

【0048】

(5) 設定情報自動バッチがクライアントPCにダウンロードされたことにより処理がクライアントPCに移り、クライアントPCは、設定情報自動バッチの処理を開始し、設定情報格納ファイルに設定情報が格納済みであるか否かを判定する(ステップ409、410)。

【0049】

(6) ステップ 4 1 0 の判定で、設定情報格納ファイルに設定情報が格納済みでなかった場合、設定情報格納ファイルに設定情報を追加して処理を終了する（ステップ 4 1 1）。

【 0 0 5 0 】

(7) ステップ 4 1 0 の判定で、設定情報格納ファイルに設定情報が格納済みであった場合、ダウンロードしたバッチ内の設定情報と自 P C 内の設定情報とを比較し、設定情報内容に変更があったか否かを判定する（ステップ 4 1 2）。

【 0 0 5 1 】

(8) ステップ 4 1 2 の判定で、設定情報内容に変更がなかった場合、そのまま処理を終了し、設定情報内容に変更があった場合、自 P C 内の設定情報格納ファイルの設定情報を更新して処理を終了する（ステップ 4 1 3）。

【 0 0 5 2 】

前述の処理は、クライアント P C が 1 企業 1 利用の場合であったが、次に、クライアント P C が 1 企業複数利用の場合の処理を図 5 に示すフローを参照して説明する。ここで図示しているフローは、前述した設定情報自動バッチがダウンロードされた後のクライアント P C での処理である。

【 0 0 5 3 】

(1) 設定情報自動バッチがクライアント P C にダウンロードされたことにより、クライアント P C は、設定情報自動バッチの処理を開始し、設定情報格納ファイルに設定情報が格納済みであるか否かを判定する（ステップ 4 0 9、4 1 0）。

【 0 0 5 4 】

(2) ステップ 5 0 2 の判定で、設定情報格納ファイルに設定情報が格納済みでなかった場合、設定情報格納ファイルに設定情報を追加して処理を終了する（ステップ 5 0 3）。

【 0 0 5 5 】

(3) ステップ 5 0 2 の判定で、設定情報格納ファイルに設定情報が格納済みであった場合、設定情報格納ファイルの設定情報を利用者毎の設定情報に更新して処理を終了する（ステップ 5 0 4）。

【0056】

図6は専用プログラムのVR管理の処理動作を説明するフローチャートであり、以下、これについて説明する。

【0057】

(1) クライアントPCにおいて専用プログラムが起動され、専用プログラムVR管理処理が開始されると、クライアントPCは、まず、サーバに対して、VRの問い合わせを送信する(ステップ601、602)。

【0058】

(2) サーバは、クライアントPCからの問い合わせを受け取ると、自サーバ内に管理しているVR情報を取り出して、応答情報としてVR情報をクライアントPCに送信する(ステップ603、604)。

【0059】

(3) クライアントPCは、応答情報としてのVR情報を受け取り、自PC内で管理しているVR情報と応答されたVR情報とが一致しているか否かを判定する(ステップ605、606)。

【0060】

(4) ステップ606での判定で、両VRが一致していた場合、ここでの処理を終了し、不一致であった場合、新たなVRを持つ専用プログラムをダウンロードして、ここでの処理を終了する(ステップ606、607)。

【0061】

図7はクライアントPCからサーバへファイルを伝送するファイルのアップロード処理を説明するフローチャートであり、以下、これについて説明する。

【0062】

(1) クライアントPCでファイルのアップロード処理を開始させると、PC内の専用プログラムは、PC内の転送ファイル16から指定されたファイルを読み込み、データ圧縮・組立てを行う。この処理は、データ量が分割サイズになるか、データに含まれるファイルの終了(EOF)が検出できるまで続けられる(ステップ701~703)。

【0063】

(2) ステップ703で、データ圧縮・組立てが分割サイズなった場合、または、ファイル終了を検出した場合、そのファイルデータをサーバに送信し、サーバからの受信の応答を受信する(ステップ704)。

【0064】

(3) 送信したデータにファイルの終了(EOF)を示す情報が含まれていたか否かを判定し、ファイルの終了(EOF)を示す情報が含まれていなかった場合、ステップ702の処理に戻って、ファイルの次の分割サイズの情報についての処理を続け、ファイルの終了(EOF)を示す情報が含まれていた場合、指示されたファイルの送信が終了しているので、クライアントPCでの処理を終了する(ステップ705)。

【0065】

(4) 一方、サーバは、前述のステップ704の処理でクライアントPCから送信されてくるファイルデータを受信し、そのデータを分解解凍して自サーバ内の転送ファイル36に書き込むと共に、そのデータのチェックポイントをチェックポイント格納ファイル708に格納する(ステップ706、707)。

【0066】

(5) 転送ファイル36に格納したファイルデータにファイルの終了(EOF)を示す情報が含まれていたか否かを判定し、ファイルの終了(EOF)を示す情報が含まれていなかった場合、ステップ706の処理に戻って、ファイルの次の分割サイズのデータの受信を続け、ファイルの終了(EOF)を示す情報が含まれていた場合、ファイル全体の受信が終了したことになるので、サーバでの処理を終了する(ステップ709)。

【0067】

図8はサーバからクライアントPCへファイルを伝送するファイルのダウンロード処理を説明するフローチャートであり、以下、これについて説明する。

【0068】

(1) クライアントPCでファイルのダウンロード処理を開始させると、PC内の専用プログラムは、サーバに対してファイルの内容を指定してファイルのダウンロードを要求する(ステップ801、802)。

【0069】

(2) サーバは、このファイルのダウンロード要求を受け取ると、自サーバ内の転送ファイル36から指定されたファイルを読み込み、データ圧縮・組立てを行う。この処理は、データ量が分割サイズになるか、データに含まれるファイルの終了(EOF)が検出できるまで続けられる(ステップ803、804)。

【0070】

(3) ステップ804で、データ圧縮・組立てが分割サイズなった場合、または、ファイル終了を検出した場合、そのファイルデータをサーバに送信し、サーバからの受信の応答を受信する(ステップ805)。

【0071】

(4) その後、サーバは、送信したデータのチェックポイントをチェックポイント格納ファイル708に格納し、送信したファイルデータにファイルの終了(EOF)を示す情報が含まれていたか否かを判定し、ファイルの終了(EOF)を示す情報が含まれていなかった場合、ステップ803の処理に戻って、ファイルの次の分割サイズのデータに対する処理を続け、ファイルの終了(EOF)を示す情報が含まれていた場合、ファイル全体の送信が終了したことになるので、サーバでの処理を終了する(ステップ806、807)。

【0072】

(5) 一方、クライアントPCは、前述のステップ805の処理でサーバから送信されてくるファイルデータを受信し、そのデータを分解解凍して自PC内の転送ファイル16に書き込む(ステップ809、810)。

【0073】

(6) 転送ファイル16に格納したファイルデータにファイルの終了(EOF)を示す情報が含まれていたか否かを判定し、ファイルの終了(EOF)を示す情報が含まれていなかった場合、ステップ809の処理に戻って、ファイルの次の分割サイズのデータの受信を続け、ファイルの終了(EOF)を示す情報が含まれていた場合、ファイル全体の受信が終了したことになるので、クライアントPCでの処理を終了する(ステップ811)。

【0074】

前述で説明したファイルのアップロード、ダウンロードの際に、伝送中のデータには、データ抜け、改竄防止のためにチェックディジットビットが付加されて伝送される。また、チェックポイントとしては、分割したファイルデータに、順に付与される分割番号等を用いればよい。

【 0 0 7 5 】

図 9 はアップロード時に障害が発生した場合のチェックポイントからのファイル再送の処理を説明するフローチャートであり、以下、これについて説明する。ここでの処理は、図 7 のフローにおけるステップ 7 0 4、7 0 6 の処理で、クライアント PC がデータを送信しサーバからの応答を受けてデータの伝送を行っている途中で、障害の発生等によりサーバからの応答が得られなくなったときの処理である。

【 0 0 7 6 】

(1) クライアント PC の専用プログラムは、ファイルデータの伝送の途中で障害の発生を検出すると、チェックポイントからの再送処理を開始し、まず、サーバに対して、再送すべきチェックポイントの取得の要求を送信する (ステップ 9 0 1、9 0 2)。

【 0 0 7 7 】

(2) チェックポイントの取得要求を受け取ったサーバは、障害発生前までに受信しているファイルデータのチェックポイントを格納管理している格納ファイル 7 0 8 からチェックポイントを読み込んで、クライアント PC に応答する (ステップ 9 0 3)。

【 0 0 7 8 】

(3) サーバから送信されてきたチェックポイントを受信したクライアント PC は、再送チェックポイントを取得できたので、その再送チェックポイントを転送ファイル 1 6 の読み込みポイントに設定する (ステップ 9 0 5)。

【 0 0 7 9 】

(4) その後、図 7 により説明したステップ 7 0 2 ~ 7 0 9 の処理の場合と同様の処理を続ける (ステップ 7 0 2 ~ 7 0 9)。

【 0 0 8 0 】

図10はダウンロード時に障害が発生した場合のチェックポイントからのファイル再送の処理を説明するフローチャートであり、以下、これについて説明する。ここでの処理は、図7のフローにおけるステップ805、809の処理で、サーバがデータを送信しクライアントPCからの応答を受けてデータの伝送を行っている途中で、処理の発生等によりサーバからのデータが得られなくなったときの処理である。

【0081】

(1) クライアントPCの専用プログラムは、ファイルデータの伝送の途中で障害の発生を検出すると、チェックポイントからの再送処理を開始し、まず、サーバに対して、再送すべきチェックポイントの取得の要求を送信する(ステップ101、102)。

【0082】

(2) チェックポイントの取得要求を受け取ったサーバは、障害発生前までに受信しているファイルデータのチェックポイントを格納管理している格納ファイル708からチェックポイントを読み込んで、クライアントPCに応答する(ステップ103)。

【0083】

(3) サーバから送信されてきたチェックポイントを受信したクライアントPCは、再送チェックポイントを取得できたので、その再送チェックポイントを転送ファイル16の書き込みポイントに再設定し、その再送チェックポイントからのファイルデータの再送をサーバに要求する(ステップ104～106)。

【0084】

(4) ファイルデータの再送要求を受けたサーバは、再送チェックポイントを転送ファイル36の読み込みポイントに設定する(ステップ107)。

【0085】

(5) その後、図8により説明したステップ703～811の処理の場合と同様の処理を続ける(ステップ702～709)。

【0086】

前述した本発明の実施形態による処理は、処理プログラムを構成してそのプロ

グラムを実行することにより行うことができ、また、その処理プログラムは、H D、D A T、F D、M O、C D-R O M等の記録媒体に格納して提供することができる。

【0087】

前述した本発明の実施形態は、ファイルデータの伝送をH T T P Sプロトコルを使用して行うようにしているので、伝送するファイルデータが暗号化され盗聴を防止することができ、F T Pプロトコルを通過させないネットワーク構成を取っているので、不特定多数の第三者からのサーバへの攻撃を防止することができるという効果を得ることができる。

【0088】

また、前述した本発明の実施形態は、クライアントP Cにファイルデータ伝送のための専用プログラムを持ち、伝送するファイルデータを圧縮しているので、伝達スピードの向上を図ることができ、伝送するファイルデータを一定のサイズに分割して送信することとしているので、サーバ側のアプリケーションプログラムが、1回のデータ受信でメモリに常駐する時間を、ファイルの大きさに関係なく、一定時間内に納めることができ、かつ、障害発生時に備えて、再送用のチェックポイントを設けているため、不安定なインターネットの通信で、再度、先頭からデータ送信する必要をなくすことができるという効果を得ることができる。

【0089】

さらに、前述した本発明の実施形態は、伝送中のデータに、チェックディジットビットを設けているので、データ抜け、データの改竄等を防止することができるという効果を得ることができる。

【0090】

また、前述した本発明の実施形態は、専用プログラムをマルチプラットフォームに対応させているので、プラットフォーム毎に、専用プログラムを持つ必要をなくすことができ、専用プログラムをクライアントP Cのオペレーションの延長でサーバからダウンロードして使用可能にしているので、ユーザによるインストール等の手間を発生させることがないという効果を得ることができる。

【0091】

【発明の効果】

以上説明したように本発明によれば、不安定がちなインターネットを使用して、クライアントPCで、特別な操作をすることなく、世界的に広く普及しているHTTPSプロトコルを使用し、かつ、長大ファイルの送受信を高い信頼性を持って効率よく行うことができる。

【図面の簡単な説明】

【図1】

本発明の一実施形態によるファイル伝送システムの全体の構成を示すブロック図である。

【図2】

専用プログラムの動作環境の設定について説明する図である。

【図3】

専用プログラムのダウンロードについて説明する図である。

【図4】

クライアントPCが1企業1利用の場合の専用プログラム動作環境設定の処理動作を説明するフローチャートである。

【図5】

クライアントPCが1企業複数利用の場合のクライアントPCでの専用プログラム動作環境設定の処理動作を説明するフローチャートである。

【図6】

専用プログラムのVR管理の処理動作を説明するフローチャートである。

【図7】

クライアントPCからサーバへファイルを伝送するファイルのアップロード処理を説明するフローチャートである。

【図8】

サーバからクライアントPCへファイルを伝送するファイルのダウンロード処理を説明するフローチャートである。

【図9】

アップロード時に障害が発生した場合のチェックポイントからのファイル再送

の処理を説明するフローチャートである。

【図 1 0】

ダウンロード時に障害が発生した場合のチェックポイントからのファイル再送の処理を説明するフローチャートである。

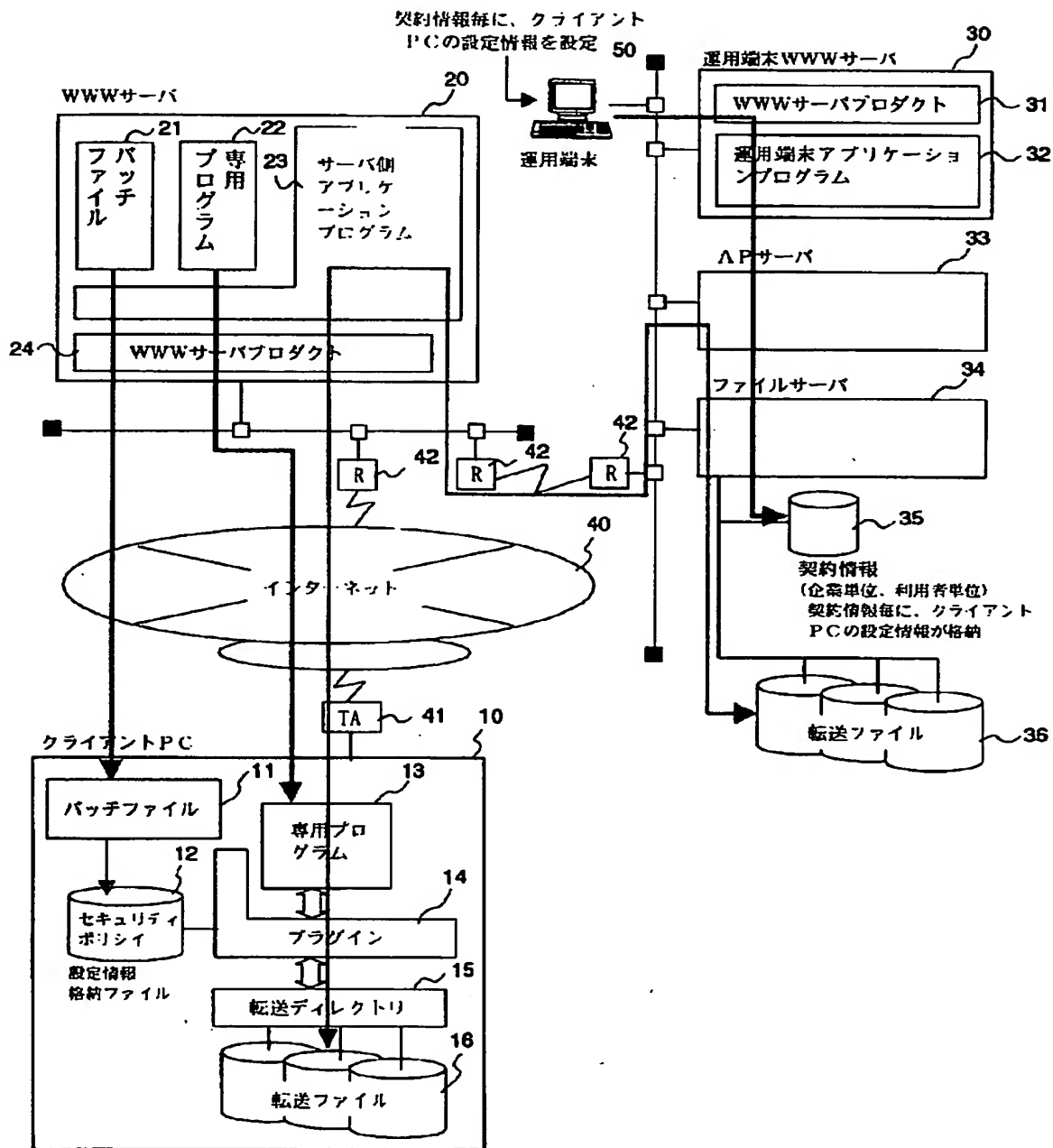
【符号の説明】

- 1 0 クライアント P C
- 1 1 バッチファイル
- 1 2 設定情報ファイル
- 1 3、2 2 専用プログラム
- 1 4 プラグイン手段
- 1 5 転送ディレクトリ
- 1 6、3 6 転送ファイル
- 2 0 WWWサーバ
- 2 1 バッチファイル
- 2 3 サーバ側アプリケーションプログラム
- 2 4 WWWサーバプロダクト
- 3 0 端末運用WWWサーバ
- 3 1 WWWサーバプロダクト
- 3 2 運用端末アプリケーション
- 3 3 アプリケーション (A P) サーバ
- 3 4 ファイルサーバ
- 3 5 契約情報ファイル
- 4 0 インターネット
- 4 1 ターミナルアダプタ
- 4 2 ルータ (R)
- 5 0 運用端末

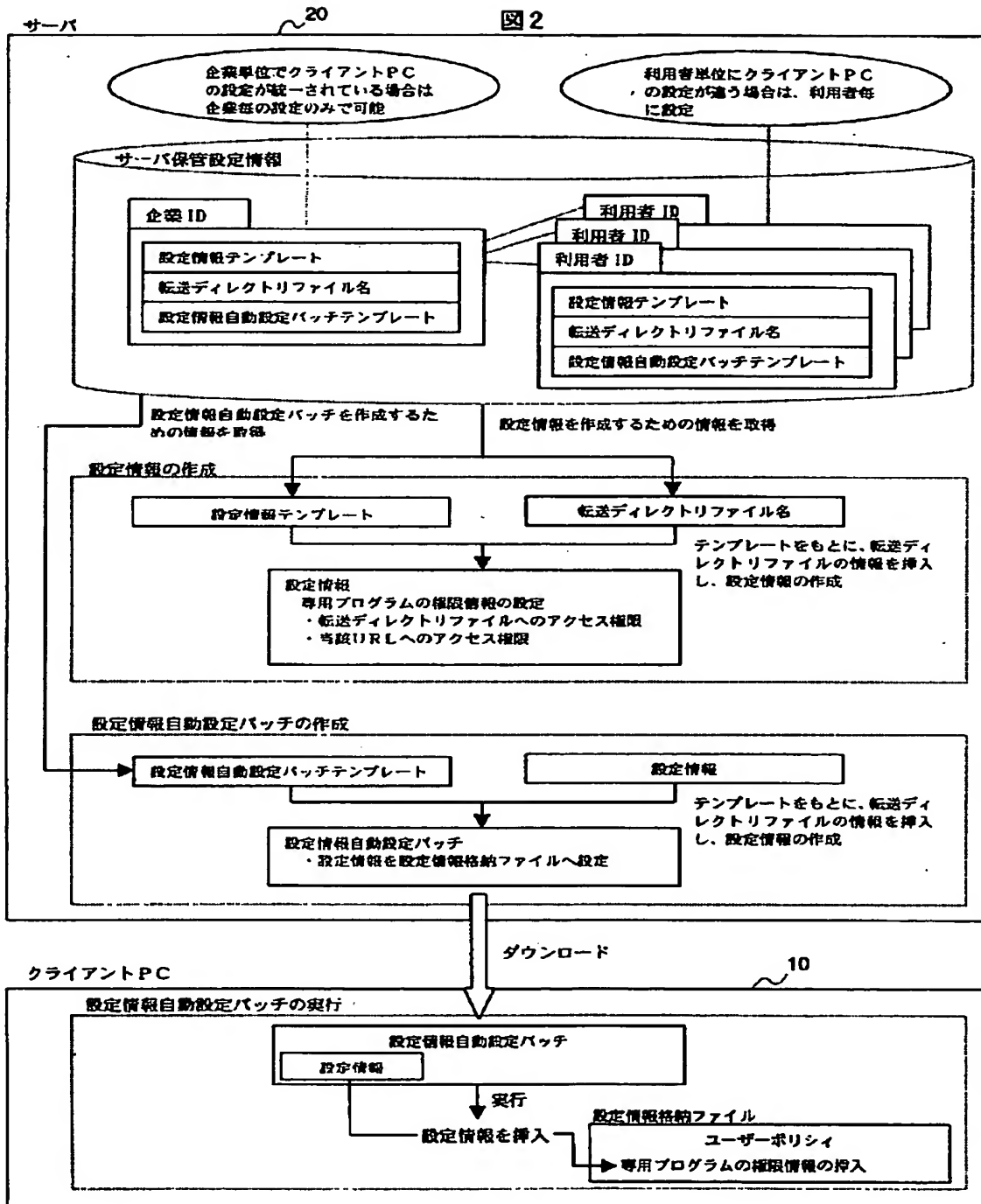
【書類名】 図面

【図1】

図1

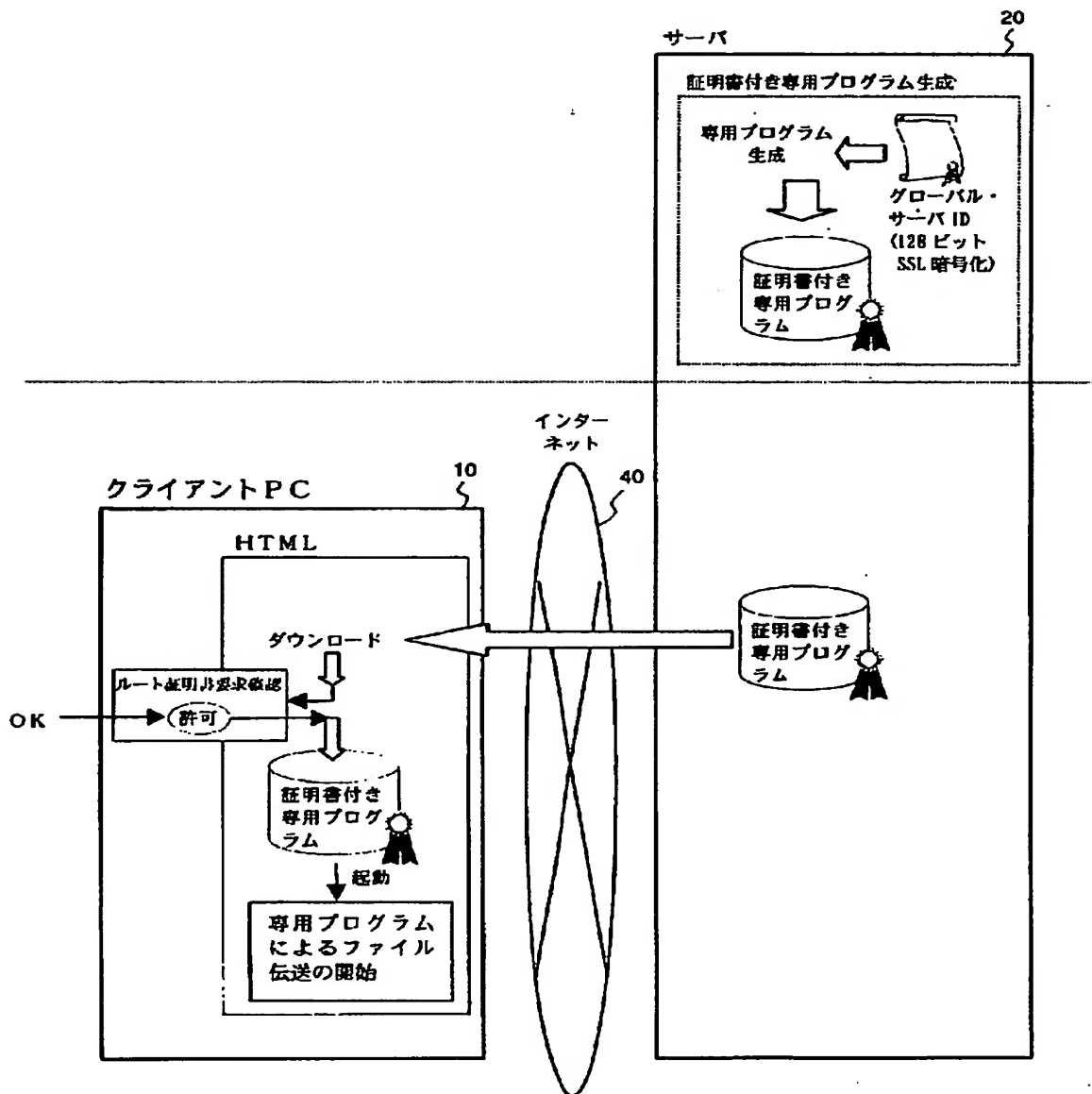


【図2】



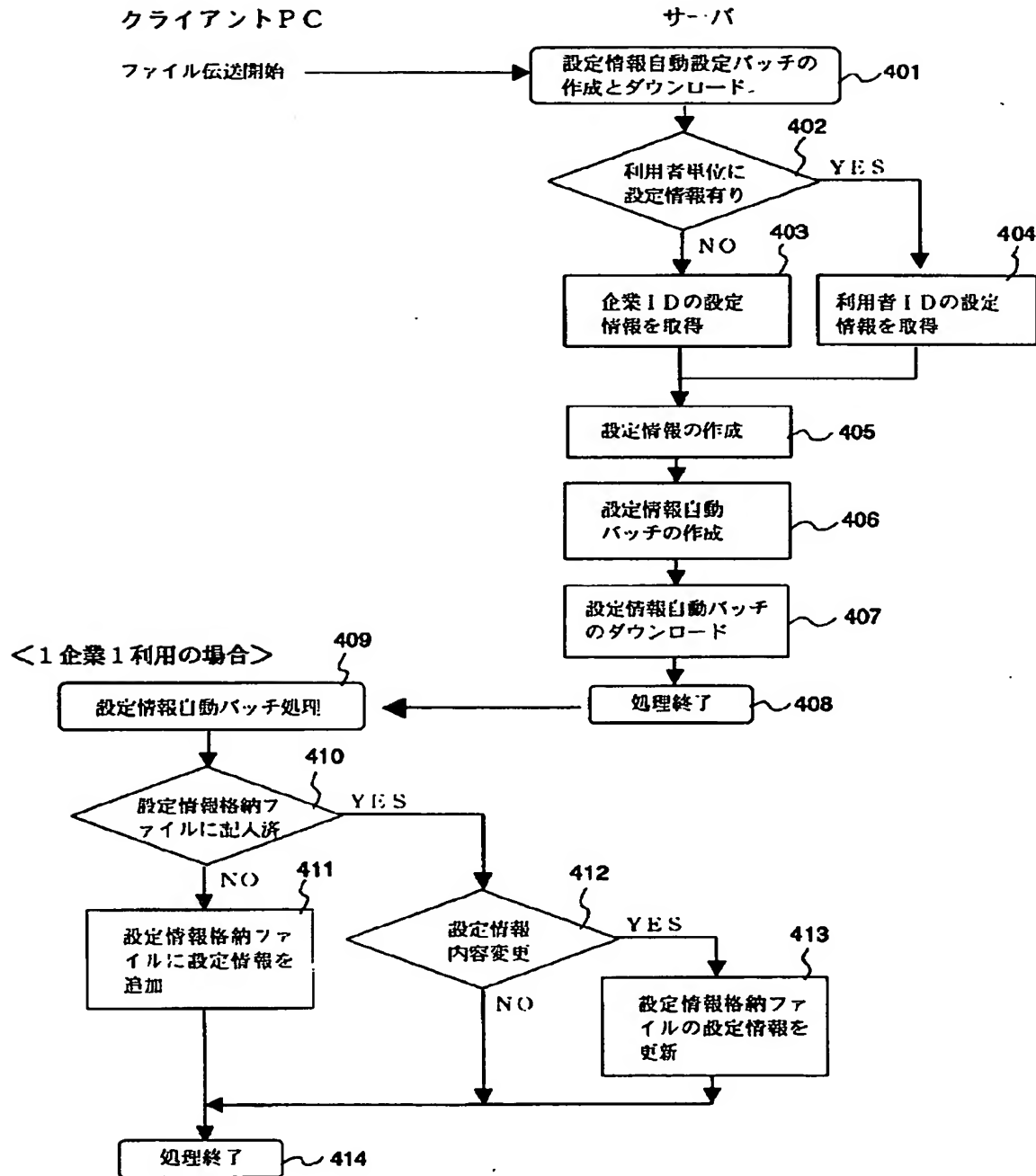
【図3】

図3



【図4】

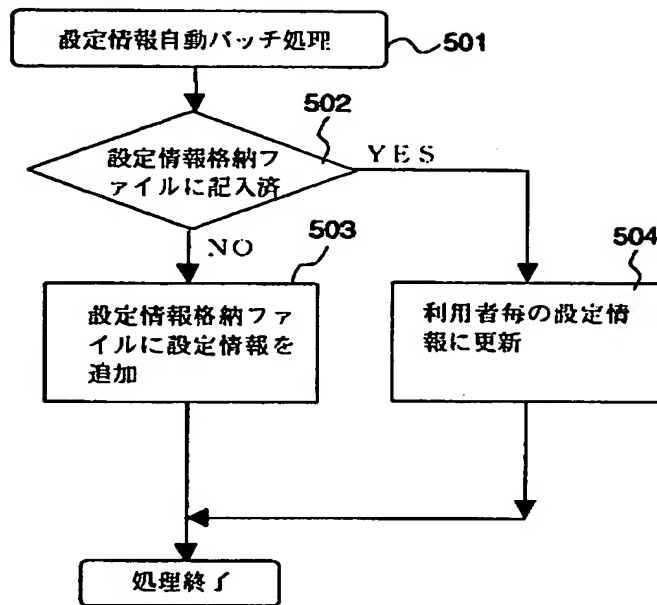
図4



【図5】

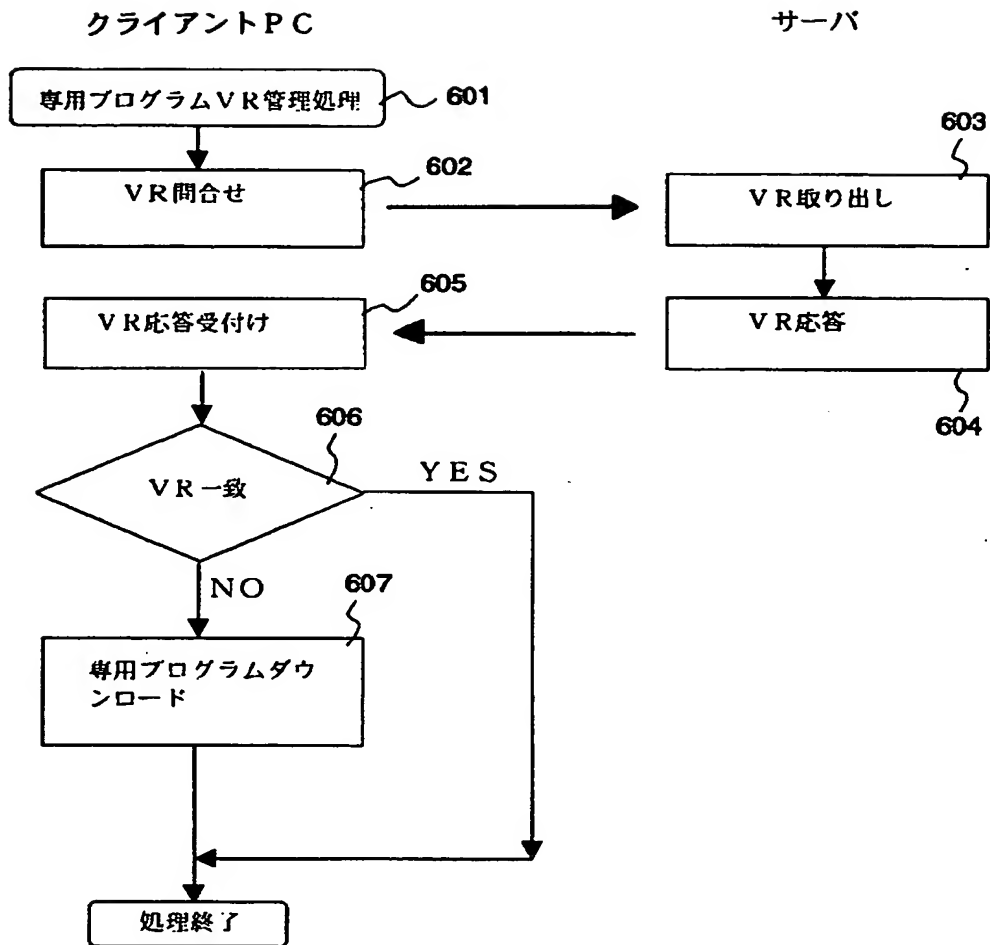
図5

<1 企業複数利用の場合>

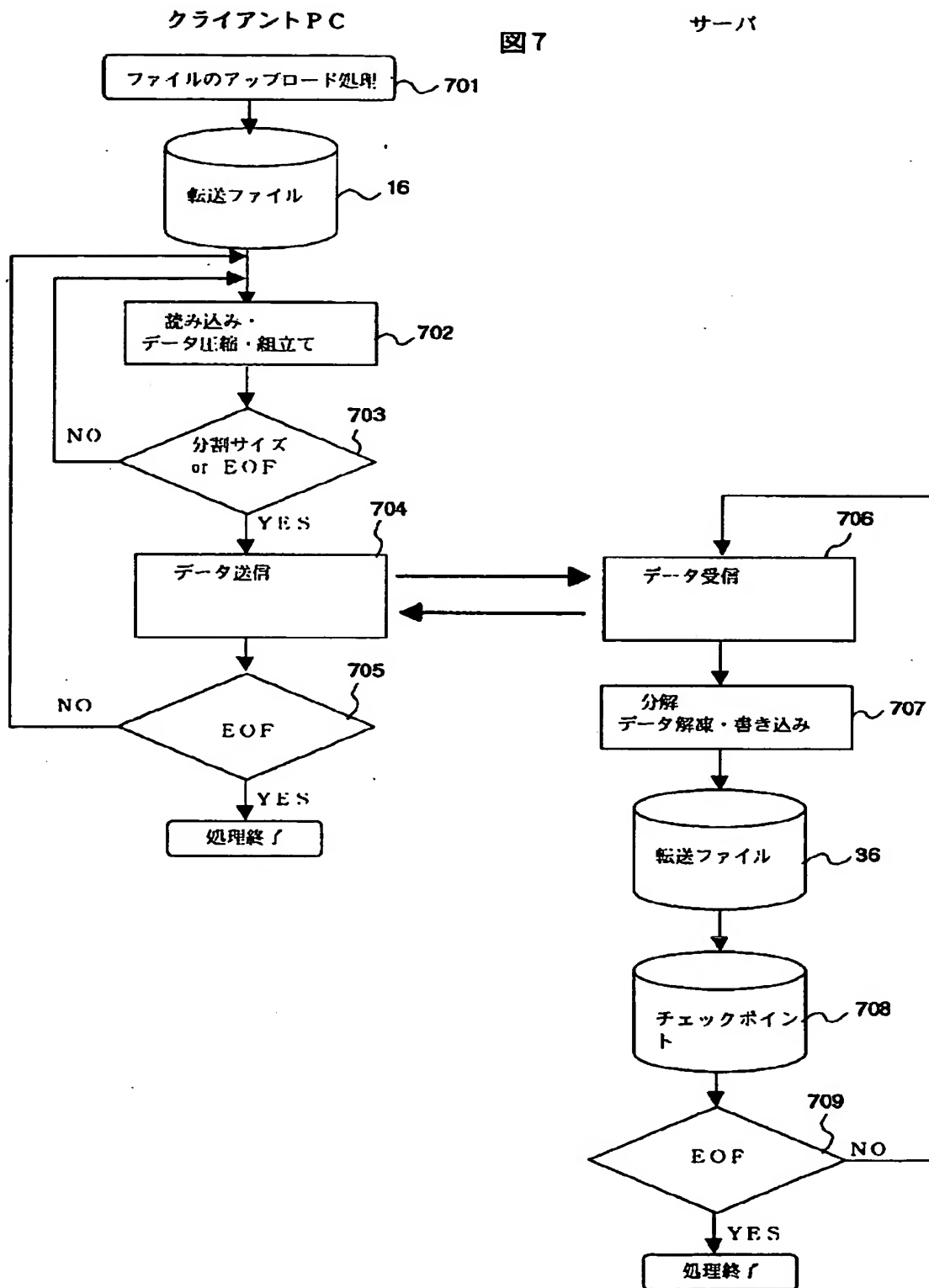


【図6】

図6

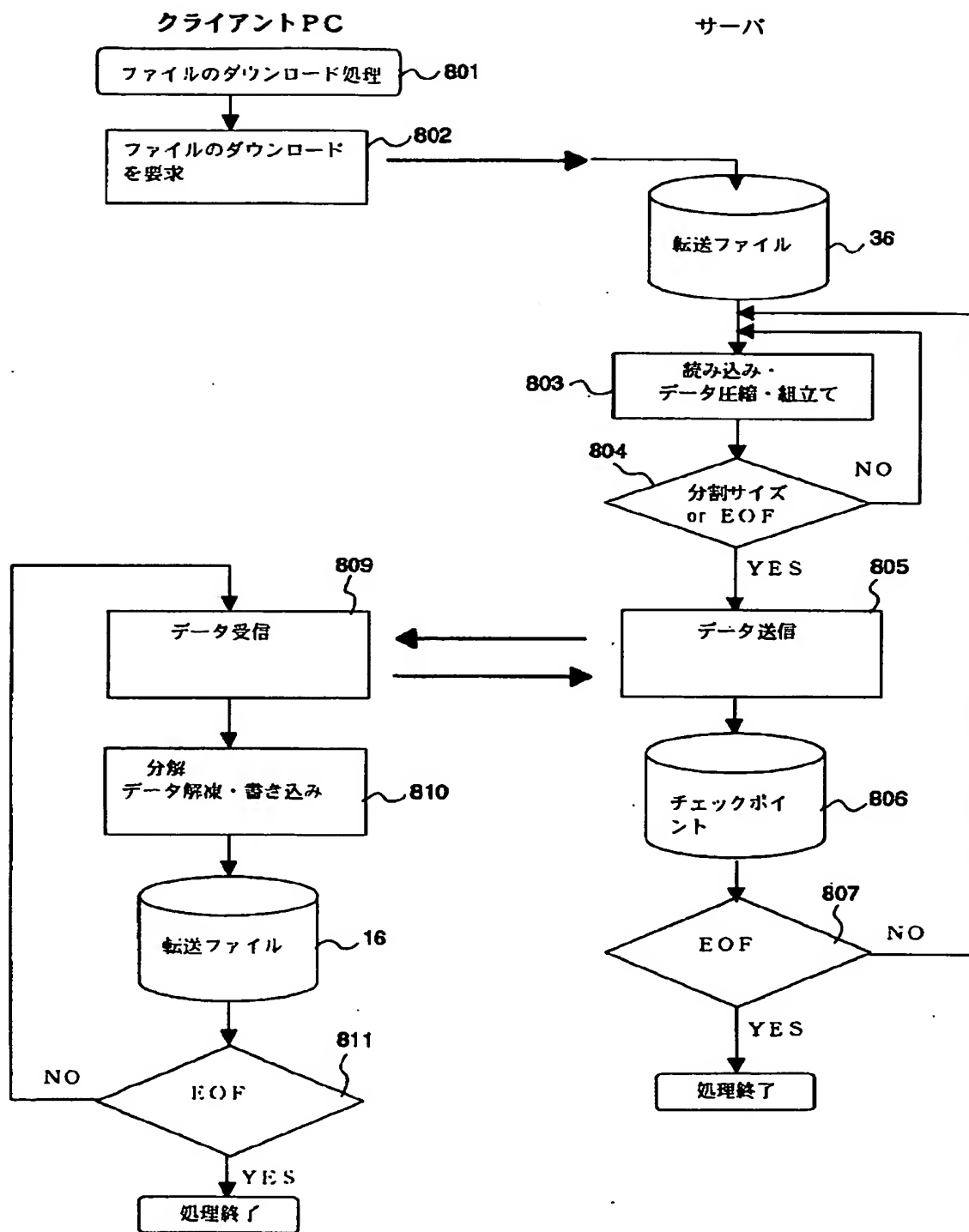


【図 7】

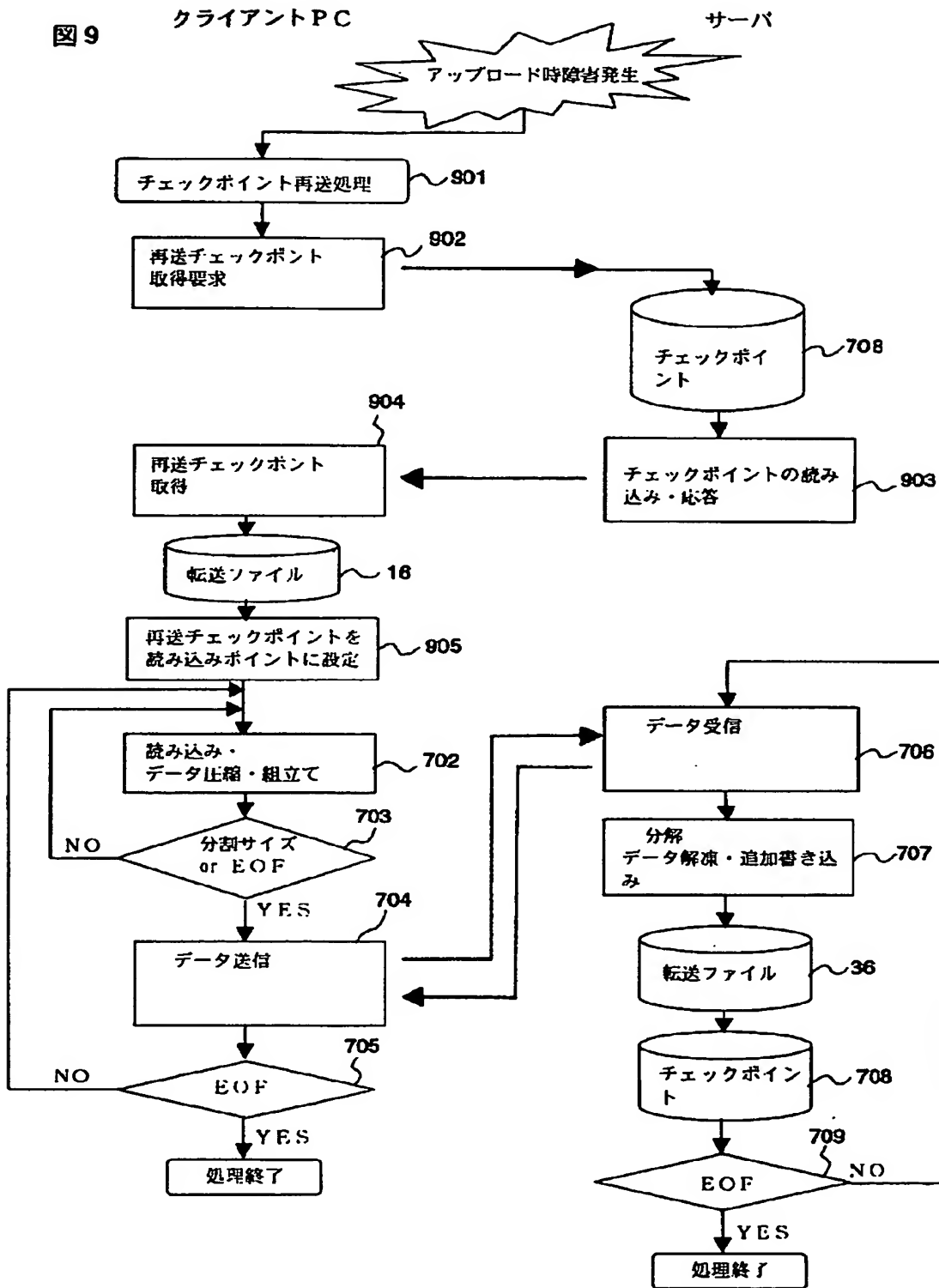


【図8】

図8

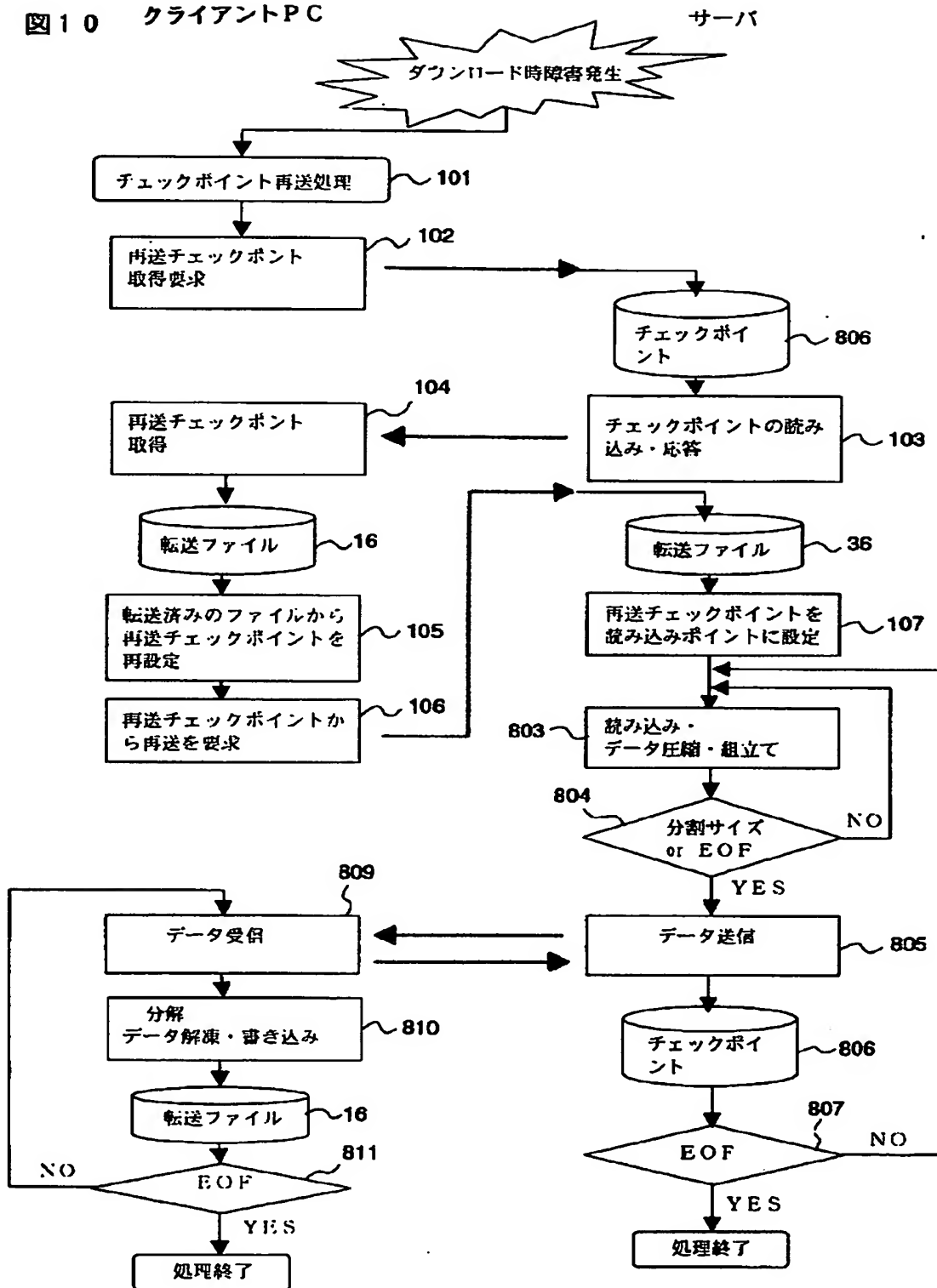


【図9】



【図10】

図10 クライアントPC



【書類名】 要約書

【要約】

【課題】 不安定がちなインターネットを用い、クライアントPCで、特別な操作をすることなく、長大ファイルの送受信を高い信頼性を持って効率よく行う。

【解決手段】 クライアントPC10と、WWWサーバ20、運用端末サーバ30、APサーバ33、ファイルサーバ34の複数のサーバを含んで構成される処理システムとがインターネット40を介して接続されている。PCとファイルサーバの転送ファイル36との間のファイルデータの伝送は、専用プログラムを用いるHTTPSプロトコルを使用して行われる。ファイルデータは、一定のサイズに分割し、かつ、圧縮して伝送される。また、障害発生に備えて、再送用のチェックポイントを設ける。専用プログラムは、マルチプラットフォームに対応させられており、PCのオペレーションの延長でサーバからダウンロードして使用可能である。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所

出 願 人 履 歴 情 報

識別番号 [391002409]

1. 変更年月日 2000年 3月30日

[変更理由] 名称変更

住 所 東京都大田区大森北3丁目2番16号

氏 名 株式会社 日立システムアンドサービス